IN THE SPECIFICATION:

The paragraph beginning at line 15 of page 13 has been amended as follows:

Printer 20 is also connected to computer 10 by connection 1 and is preferably a laser or an ink-jet printer which is capable of printing images on recording medium based on received print data. Printer 20 has a fixed storage 21 which is preferably a fixed disk, but can be another form of computer memory such as ~~ROM or EEPROM~~ read-only memory (ROM) or electrically-erasable programmable read-only memory (EEPROM). The contents of fixed storage 21 and the operation of printer 20 according to the present invention are discussed in more detail below.

The paragraph beginning at line 16 of page 16 has been amended as follows:

Although applications exist, such as PGP ("pretty good privacy"), for supporting the cryptographic signature of data and the subsequent verification of a cryptographic signature, such applications are seen to have a significant shortcoming with respect to the Microsoft Windows CAPI functionality. In particular, other cryptographic applications, such as PGP, require the user of the application to maintain the storage of the key pair that is used to create the cryptographic signature. Accordingly, such applications do not maintain the key pair under strict security and may be more prone to a security breach in which an unauthorized user of the computer can access the key pair and use it to access encrypted data of the authorized user.

The paragraph beginning at line 11 of page 17 has been amended as follows:

Returning to Figure 3, key database 50 is a component of operating system 40 and is used to securely generate and maintain user-specific key pairs for the users of computer 10. In particular, key database 50 contains a user entry for each user of computer 10, each user entry containing a corresponding user-specific key pair, such as user-specific key pair 51a ~~51~~ which is in the entry corresponding to user1 51. Each user-specific key pair contains a private key and a public key for encryption/signing of data objects and for authenticity verification of such encrypted/signed data objects. For example, user-specific key pair 51 includes user-specific public key 53 and user-specific private key 54, both of which are unique and correspond to user1 51.

Please add a new paragraph at line 27 of page 17, as follows:

Likewise, key database 50 may include entries for other users, such as user2 52 with public key 55 and private key 56.

Please add a new paragraph at line 17 of page 18, as follows:

Likewise, registry 41 may include entries for other users, such as user2 43 which includes a login ID 47 and a digital signature 46 which function in the same way as the corresponding entries for user1 42.

The paragraph beginning a line 31 of page 29 (bridging pages 29 and 30), has been amended as follows:

Next, printer test page 102 is generated at printer 20 in response to a command which is preferably provided at the front panel of printer 20 by the user of computer 10. Printer test page contains a printed hash value 103 of which is the correct hash value for printer public key 25. Printed hash value 103 is entered into computer 10 by the user and is provided to hash verification algorithm 84 along with printer public key hash value 69. Hash verification algorithm 84 determines whether the two hash values match in order to verify the authenticity of received printer public key 25. If there is a match, then computer 10 accepts printer public key 25 as an authentic copy from printer 20 and stores it into storage area 62 for subsequent use. If there is not a match, then an error message 105 is generated for display on display 11 of computer 10 to prompt the user to take action, such as sending another request to printer 20 for printer public key 25, or such as re-entering printed hash value 103 into computer 10.